FSA Integration Partner

ED PIN Re-Engineering Analysis

ED PIN Business Requirements

&

Standards

Deliverable 131.1.2

Version 1.2

July 31, 2003

Amendment History

DATE	SECTION/ PAGE	DESCRIPTION	REQUESTED BY	MADE BY
7/29/2003	All	Revisions of all sections based on 7/25 feedback session with Nina Colón	Nina Colón	Integration Partner
7/30/2003	Section 4	Organized the Business Requirements. Currently implemented requirements are listed first. Applicable footnotes have been documented as requirements where appropriate. Applicable requirements have been attributed to source(s).	Nina Colón	Integration Partner
7/31/2003	All	Grammatical changes and corrections based on comments from 7/30 meeting and initial revision.	Nina Colón	Integration Partner

Table of Contents

FEDERAL
STUDENT AID
We Help Put America Through School

FSA Integration Partner
ED PIN Re-Engineering Analysis
131.1.2 Business Requirements & Standards

1   BACKGROUND

The ED PIN process was instituted by the Department of Education Office of Federal Student Aid (FSA) in 1997. Originally designed to authenticate users utilizing the FAFSA on the Web product, the ED PIN is now leveraged across the FSA enterprise by other user-facing services that include system access and electronic signature functionality. The ED PIN processes are a CPS[1] sub-system and are also used by internal FSA organizations (such as Schools) to support Title IV federal student aid processing. The ED PIN is used to authenticate users for web-based access to various FSA systems. The ED PIN system maintains authentication data for over 32 million users and is growing at an increasing rate as more customers begin to use FSA web-based products. FSA's ability to authenticate web customers for various services is critically dependent upon the integrity and availability of the ED PIN data. The ED PIN process also needs to support the potential for increased future use through standard processes and an infrastructure that is scaleable and robust.

The ED PIN is issued to students, parents, financial aid administrators (FAAs) and FSA trading partners. The ED PIN is required for authenticating users' to access their FAFSA on the Web data or current status of processed data, access to their data stored within NSLDS[2], access to Direct Loan Servicing website functions, access to Direct Loan Consolidation website functions, as well as for electronic signature capabilities[3]. Financial Aid Administrators at institutions within Title IV programs require an ED PIN to access the functions within FAA Access Online and E-Campus Based programs. Future uses of the ED PIN currently are under consideration by FSA and may include user authentication on the FSA Student Portal.

The ED PIN Re-Engineering Analysis is a high priority (#17, FY2003) FSA initiative. The purpose of this initiative is to examine the ED PIN and its supporting processes from the perspective of future use. The term "Re-Engineering" implies an ED PIN system that incorporates the enterprise business requirements and is focused towards ensuring the infrastructure (processes, standards and technology components) can sustain proper, continued and increased usage. The ED PIN processes support Objective 5 of the Department of Education Strategic Plan – Enhance the Quality of and Access to Postsecondary and Adult Education[4].

1.1   Organization of the Document

This section provides the background for the ED PIN Re-Engineering Analysis initiative. Section 2 documents the re-engineering analysis and findings (or issues) that need to be addressed. Section 3 presents the conceptual framework for the enterprise ED PIN business processes. Section 4 documents the business requirements and associated ED PIN standards for

---

[1] Central Processing System.
[2] National Student Loan Data System.
[3] For example, Promissory Notes.
[4] U.S. Department of Education Strategic Plan 2002 – 2007.

an enterprise shared service. Section 4 also documents current implementation of the requirements. This section also identifies the requirements that will alleviate the findings noted in section 2. The conclusions of the re-engineering analysis are noted in Section 5. References are noted in Section 6. The appendices provide additional information on current ED PIN processes, systems, and interfaces, a glossary with a definition of terms used within this document, and meeting notes from interviews with FSA client system business owners.

1.2 Acknowledgements

During the analysis the team met with various FSA client system business owners. The agenda items for the meetings included (1) determination of which systems interface with the ED PIN system, (2) how the systems interface with and use the ED PIN system, (3) what type of user access is based on authentication with the ED PIN system, (4) strengths and weaknesses, or specific business requirements, and (5) capacity (ED PIN transaction volume) information. The FSA ED PIN Re-Engineering Analysis project team acknowledges the following for their noted support:

> Jeanne Saunders – Business Integration & Application Processing
> Jennifer Douglas – Business Sponsor
> Nina Colón – Project Management
> Cynthia Battle – Direct Loan Servicing functionality
> Denise Leifeste – Direct Loan Consolidation functionality
> Nina Colón, Ginger Klock, Ida Mondragon - application processing functionality
> (FAFSA on the Web, Student Access, ED PIN, FAA Access Online, CPS, STAN)
> Lynn Alexander – NSLDS functionality
> Daria Adams – Standard Student Identification Method Team
> Robert Ingwalson – Security Architecture Team
> Keith Wilson – Data Strategy Team
> Neil Sattler – Electronic Signature, STAN and E-Gov functionality

Meeting notes are attached in Appendix C of this document. Other documentation utilized to complete this analysis is noted in the reference section.

FEDERAL
STUDENT AID
We Help Put America Through School

FSA Integration Partner
ED PIN Re-Engineering Analysis
131.1.2 Business Requirements & Standards

2 ED PIN RE-ENGINEERING ANALYSIS & FINDINGS

2.1 Business Objective

The objective of the ED PIN Re-Engineering Analysis is to recommend an enterprise vision for the ED PIN system and associated upgrade plans for the system infrastructure, business processes and standards in support of FSA mission critical functions[5]. As stated in the business justification, the objective of this initiative will be attained working collaboratively with client systems.

The ED PIN Re-Engineering Analysis initiative is planned with 2 phases, (1) Requirements and Standards and (2) Technical Architecture. The requirements and standards phase is addressed in this Draft document. The second phase, Technical Architecture, will follow the completion of Phase 1. Both phases are planned to be completed by September 30, 2003.

Further elaboration on the objective of the ED PIN Re-Engineering Analysis initiative includes establishing the requirements for the ED PIN processes and sub-system to be scaleable as an enterprise wide authentication shared service for all users. This initiative is focused on developing the enterprise vision for using the ED PIN system and analyzing the architecture to support the vision; without any interruption to FSA mission critical functions.

The requirements and standards for the ED PIN system that are noted in this document include business needs recommended by FSA client business system owners utilizing the ED PIN as well as applicable Federal guidance and industry best practices.

2.2 Analysis Findings

The purpose of issuing an ED PIN by FSA is to enable web-based access to FSA systems. The basic premise of using the ED PIN, in conjunction with an individual's personal data which includes their social security number, 1st two letters of the last name, and date of birth is to successfully authenticate a web user. FSA leverages a data match with the U.S. Social Security Administration (SSA) for the purpose of validating credentials provided by a user.

The analysis of current ED PIN processes has led to the identification of 3 key areas for future focus. They include:

1. Process & Infrastructure
2. Data Administration
3. Evolving Standards

---

[5] FSA Proposed Business Justification – ED PIN Re-Engineering Analysis – FSA Priority (Number) 17, Section #2.

FEDERAL
STUDENT AID
We Help Put America Through School

FSA Integration Partner
ED PIN Re-Engineering Analysis
131.1.2 Business Requirements & Standards

(Note: Findings with the "immediate" impact pose a potential risk to business operations; findings with the "Functionality for Re-engineered Design" impact should be incorporated as requirements during the design phase of the re-engineered ED PIN system):

FINDINGS	IMPACT
Process & Infrastructure	
A. **ED PIN Users without SSA Verification.** Electronic Data Exchange Destination Point Administrator to be eligible to receive an ED PIN for purposes of accessing student data, no users in this category are subject to the SSA 3rd party verification. At present there are approximately 20,000[6] ED PINs issued to FAAs; the application credentials for these records are not validated with SSA[7].	Immediate
B. **E-signature Impact From Lack of FAA 3rd Party Verification.** Use of an ED PIN as an electronic signature in cases where no 3rd party verification is performed should be prevented since it does not conform to the FSA Electronic Signature standards.	Immediate
C. **Multiple Sources for Data Input Initiation.** The process to request an ED PIN and the collection of requisite data should be initiated within the control of the ED PIN system. While the initiation of the process at different places does not pose any problem, the asynchronous process can create the potential for data mismatch among systems.	Functionality for Re-engineered Design
D. **Inconsistent Use of ED PIN for Authentication.** The use of the ED PIN for authentication should become consistent across all the system using this function. While some systems require the use of an ED PIN to update personal (demographic) data, others (e.g., ED PIN system) do not.	Functionality for Re-engineered Design
E. **No Enterprise Process for Personal Data Updates.** A process for updates to personal (demographic) data that can be consistently applied among systems utilizing the ED PIN would be beneficial.	Functionality for Re-engineered Design

---

[6] Approximately, 8,000 have read-only access.

[7] While these application credentials are not validated with SSA, it is the responsibility of the Destination Point Administrator (DPA) to approve only valid FAA credentials and applications for an ED PIN as part of the Participation Management process.

FINDINGS	IMPACT
F. **Lack of Near Real-Time Customer Notification (Email).** Customer notification regarding their ED PIN is batch processed for both new and forgotten ED PINs. The relative speed of the process for issuance of a new ED PIN is directly dependent upon the speed of 3rd party verification with SSA. However, the capability to send notifications for forgotten ED PINs instantaneously does exist and may be available for use. It is FSA's preference to use the batch communication process, per recommendation from the policy group. The ED PIN is issued via e-mail if available or via a paper mailer if no e-mail address is recorded on the ED PIN sub-system. It is FSA's preference to issue communications via e-mail if available. Client system communication related to email address needs to be consistent.	Functionality for Re-engineered Design
G. **Potential for Increased Use of ED PIN Reminder Function.** Customer interface with FSA is cyclical. There is a capability to trigger ED PIN reminders. Such a capability could be used to facilitate increased use of FSA electronic services especially for borrowers that are graduating (for loan consolidation). ED PIN reminders could also be used to transition users without electronic access especially for customers established prior to the ED PIN era.	Functionality for Re-engineered Design
H. **Lack of Audit and History Log.** The use of an ED PIN for authentication is not recorded by the ED PIN system for either an individual or a system[8]. Given that the ED PIN is used for authentication to various FSA systems, it may be important for the ED PIN system to possess knowledge related to system use as well as to possess the capability to prevent use in certain cases.	Functionality for Re-engineered Design
I. **ED PIN Functionality Distributed.** The ED PIN functionality is distributed among various CPS sub-systems including the ED PIN, CPS, STAN, and other sub-systems (e.g., ED PIN paper mailer and ED PIN electronic mailer). It may be beneficial to consolidate the functionality into a single system given the expanded use of the ED PIN beyond its original design for FAFSA on the Web. Additionally, there are a wide range of platforms (web infrastructure and mainframe infrastructure, both within and outside the FSA Virtual Data Center) utilized to support the ED PIN processes due to the dependence upon the various CPS sub-systems. For purposes of	Functionality for Re-engineered Design

---

[8] Use of the ED PIN as an electronic signature is tracked through STAN.

FINDINGS	IMPACT
future flexibility, it may be important to consider consolidating the ED PIN functionality.	
J. **Restricted Use for ED PIN of Title IV Programs.** There is no process for use of the ED PIN outside Title IV processes. The potential use of the ED PIN as part of the E-Gov pilot for Title VII and Title VIII financial aid processes presents a need for such scalability.	Functionality for Re-engineered Design
K. **Different Implementation of Electronic Signatures for FAFSA on the Web.** While the ED PIN is used for electronic signature of a FAFSA application completed electronically via FAFSA on the Web the manner in which that is performed is different from other electronic signatures (e.g., promissory notes). It would be appropriate to note specific FSA decisions authorizing such situations.	Immediate
L. **Lack of Formal Systems Impact Communication between ED PIN and Client Systems.** There is no formal vehicle between the ED PIN processes and user systems for communicating impact analyses from updates in one to other(s).	Immediate
Data Administration	
M. **Duplicative ED PIN Records.** At the time of this analysis[9] there are 34,045,807 records within this repository. Of these records, there are 5,889,575 records without an ED PIN. There are 1,270,771 duplicative records within the repository. These duplicative records mean that an individual user may have more than one ED PIN that may be used for FSA transactions.	Immediate
N. **Lack of History Log.** The ability to maintain record history associated with changes to name and DOB may be relevant as the ED PIN system grows. This will prevent any change to personal (demographic) data from generating a new ED PIN record. The current practice creates the potential for duplicate records based on a single social security number and the potential for multiple ED PINs for a customer all of which are valid. The practice of record history will also allow an activity log of data changes or updates either directly by a customer or indirectly through another FSA system.	Functionality for Re-engineered Design

---

[9] Data as of July 31st, 2003.

FINDINGS	IMPACT
Demographic data can also be validated for currency with other FSA repositories. The SSIM (Standard Student Identification Methodology) guidance may be helpful to identify and resolve The CPS and DL Servicing system provide updates to address.	
O. Lack of "Role" Data. For future uses, the ED PIN should also maintain role information associated with the user data. This is particularly important since some ED PINs are issued to non-borrowers.	Immediate

Evolving Standards

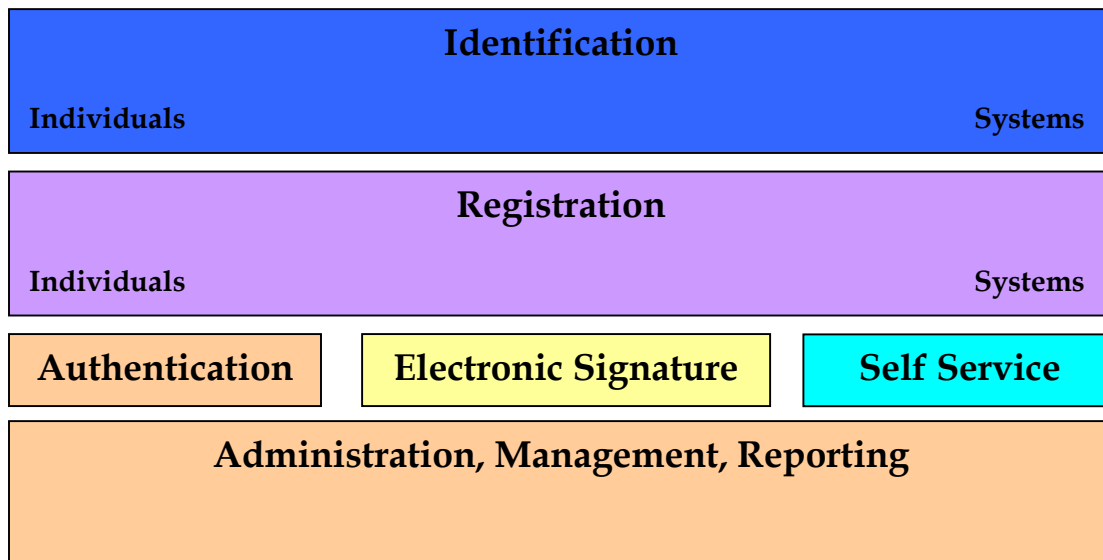|	
P. Multiple ED PIN Access Mechanisms. Access to the ED PIN infrastructure is available through 3 mechanisms - a standard Application Programming Interface (API), stored procedure calls to the ED PIN database, and through a web services option (in addition to the internal communications with CPS via FTP). Encryption standards are utilized to support ED PIN processes. Selection criteria and guidance for multiple access methods may be beneficial. Multiple access methods may also present risks for compliance with current and evolving Federal and industry authentication standards. A repository of knowledge associating the use of particular access methods by the various systems (both within and outside FSA) utilizing the ED PIN processes would also be helpful. While web services[10] technology can alleviate some of these issues, the implementation of web services should be in conjunction with the infrastructure to support publishing of the web service (internally within FSA or externally) as well as functionality to monitor the availability, response time, and maintenance of the web service in compliance with enterprise standards. Implementation of web services technology without a standard enterprise infrastructure can expose FSA to IT security risks and is not recommended. Standards will continued to evolve and the need for the infrastructure to be flexible for incorporating future standards should also be considered.	Functionality for Re-engineered Design

---

[10] The FSA web services strategy is planned under a separate initiative.

3 ED PIN PURPOSE AND FUNCTION

The purpose of the ED PIN processes is to provide a web-based mechanism to authenticate users. Based on this authentication process, users can access their data related to Title IV FSA services as well as conduct transactions requiring electronic signatures[11]. This authentication function is performed when web-based Title IV services request user credentials (SSN, 1st 2 characters of the last name and date of birth) and their ED PIN. These credentials along with the ED PIN are communicated securely to the ED PIN system which provides an authentication response.

The framework noted below is used for illustrating the major components of the enterprise authentication shared service. It is a conceptual framework for analytical purpose and does not represent a re-engineering design.

ED PIN Enterprise Authentication Framework

Identification	
Individuals	Systems

Registration	
Individuals	Systems

Authentication	Electronic Signature	Self Service

Administration, Management, Reporting

Users of the ED PIN system functionality (i.e., authentication and electronic signature) include both individual users as well as other systems/business processes. The ED PIN functionality needs to be supported with information identifying all users (i.e., individuals and systems/business processes). The information needed by the ED PIN sub-system to effectively service the authentication needs requires knowledge of users.

---

[11] Or other use as explicitly authorized by the Department.

FEDERAL
STUDENT AID
We Help Put America Through School

FSA Integration Partner
ED PIN Re-Engineering Analysis
131.1.2 Business Requirements & Standards

3.1 Identification

The Identification function refers to the data collection activities necessary for ensuring all requisite information is known prior to issuance of the ED PIN. Key data elements for both individual users and systems[12] that use the ED PIN for authentication are illustrated below.

Identification	
Individuals	**Systems**
- Social Security Number - First Name - MI - Last Name - Date of Birth - Street Address - City - State - Zip Code - E-Mail Address - Security Pass-Phrase - Other items to possibly consider include gender, country, mailing vs. permanent address, driver's license, etc. Also open to consideration, required fields in addition to SSN, Last Name, DOB.	- Name - Owner - Technical Requirements - 24 X 7 Contact(s) - System Security Officer - Production Date - ED PIN functions used in addition to authentication (Functions may include authentication request, bulk processing of ED PIN registration, ED PIN update capabilities, deactivation request, etc.) - ED PIN Authentication Mechanism (Standard API, Stored Procedure, Web Service, etc.) - Number of transactions per function per day/week/month/year - Maximum response time acceptable per function - Utilization hours - Transaction peak hours - Transactions peak load during peak hours - Average transaction load during utilization hours - Batch window (if applicable) - Test Information - Maximum Transactions

3.2 Registration

The Registration function is associated with the verification of the information provided in the previous function and the controls associated with the generation and communication of the ED PIN to users.

---

[12] Currently no formal system information is collected.

Registration	
Individuals - Edits - 3rd Party Verification with SSA - Other 3rd Party Verification requirements - Approval/Rejection & Communication to User - Issuance of ED PIN	**Systems** - Account Frequency - Report Frequency

Registered users and systems may then use the ED PIN for authentication and other approved functions.

3.3 Authentication

The Authentication function is focused at systems' use of the ED PIN for authentication.

Authentication
Access Mechanism Types - Stored Procedures - Standard API - Web Service - Ability to verify if an authentication request is originating from the   system it claims to come from - Ability to verify if a system is the intended recipient for an authentication request

3.4 Electronic Signature

Electronic Signature
The Electronic Signature function is available to individual users specifically through FSA applications and other systems. This function will comply with the FSA E-Sign standards.

3.5 ED PIN Self-Service

The ED PIN Self-Service capability allows users[13] and system owners[14] to provide updates to their information. Representative updates are noted below.

<table>
<tr><td colspan="2" align="center">Self Service</td></tr>
<tr><td>Individual
 - Change ED PIN
 - Request/Forgotten ED PIN (May want to institute revolving set of challenge questions in addition to SSN, 1st 2 characters of LN and DOB)forgotten ED PIN)
 - Update ED PIN information – All user data except SSN, DOB and Last Name (May need to include First Name as required field for new issuance of ED PIN pending final guidance and impact analysis from SSIM enterprise initiative)
 - Disable/Enable ED PIN</td><td>System Owners
 - Authorized delegated administration functions</td></tr>
</table>

3.6 Administration, Management and Reporting

The Administration, Management and Reporting function provides the capability for the various tasks necessary to maintain the system. These tasks may include the following:

<table>
<tr><td align="center">Administration, Management, Reporting

    ■   Customer Account Administration
    ■   Data Authentication/Integrity
    ■   Information Flow Policy
    ■   Information Flow Controls
    ■   Management of Security Attributes of Users allowing for separation of duties
    ■   Other automated reporting functions may include the generation of alerts and/or triggers for management attention (Currently Not Available)</td></tr>
</table>

---

[13] This capability is currently available.

[14] Currently unavailable.

4 DRAFT BUSINESS REQUIREMENTS AND STANDARDS

The business requirements and standards noted during the analysis are documented in the table below. The table also identifies the current implementation of the requirement /standard.

The draft requirements were compiled through interviews with the FSA business process owners and clients, best practices and guidelines from NIST[15] and current system documentation. The business process owners interviewed during the analysis[16] include the ED PIN and the following:

- Central Processing System (CPS)
- FAFSA on the Web (FOTW)
- FAA Access Online
- Student Authentication Network (STAN)
- E-Gov E-Authentication (FSA Team)
- National Student Loan Data System (NSLDS)
- Direct Loan Servicing
- Direct Loan Consolidation
- Security Architecture

It should be noted that not all of the requirements and standards noted below will be implemented as part of the re-engineering effort and that FSA will decide the final requirements and standards. It should also be noted that the lack of implementation of a requirement does not imply a problem with the current ED PIN system. While the table below notes whether a requirement is available as current functionality, there is also a cross-reference to the findings noted in Section 2 of this document.

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
1	The ED PIN system is an authentication facility and not an identity management system.	✓		ISO / IEC
2	Other FSA client systems authorized to use the ED PIN for authentication and subsequent granting of any type of access or information on the basis of the ED PIN will document this capability.	✓		FSA

---

[15] National Institute of Standards and Technology.
[16] Appendix C contains the meeting minutes.

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
3	The ED PIN system will incorporate the Generally Accepted System Security Principles (GASSP) as adopted by the Department. These principles will include pervasive principles that address Confidentiality, Integrity and Availability. Additionally, the ED PIN system will support protection against discovery and misuse of identity by other users – i.e., Anonymity (user can use a resource without disclosing the user's identity to other users), Pseudonymity (user's identity is not disclosed to other users but the user is still accountable for its action), Unlinkability (user can use a resource multiple times without other users being able to link these sessions to each other), and Unobservability (user can utilize a resource without unauthorized parties being able to observe his/her actions or usage).	✓		NIST
4	The ED PIN system will conform to the FSA Security Architecture.	✓		FSA
5	The ED PIN access credential establishes user accountability and is used to prevent unauthorized people or processes from entering an FSA IT system (resource).	✓		NIST
6	The ED PIN access credential is used by users for access to user data maintained in FSA IT systems.	✓		ISO / IEC
7	The ED PIN credential is not required for general access to FSA resources where no transactions are conducted and there is no privacy, confidential or other personal or sensitive data.	✓		NIST
8	Any access to the ED PIN user data by other than the user is not permitted, including for system tests.	✓		ISO / IEC
9	It is the responsibility of authorized FSA systems utilizing the ED PIN for user authentication to test the functionality in coordination with the ED PIN system owner.	✓		FSA
10	The ED PIN is required by users interfacing with FSA via the Internet to identify them uniquely before being allowed to perform any transactions on FSA systems.	✓		FSA

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
11	The ED PIN will not provide authorization functionality for any FSA client system. Any authorizations (or role-based access) are the responsibility of the client system. Client systems may grant varying levels of authorization to users on the basis of ED PIN authentication.	✓		FSA
12	The ED PIN will provide an enterprise shared service for authentication that can be used by FSA client systems. The ED PIN will not link actions to specific users except for ED PIN functionality – registration, ED PIN management, and electronic signature functions.	✓		FSA & ISO / IEC
13	The ED PIN will support the FSA Electronic Signature standards consistently. The electronic signature standards are implemented per the Student Authentication Network Functional Specification.	✓		FSA
14	The ED PIN architecture will integrate with the FSA Integrated Technical Architecture and include the appropriate redundancy, backup and recovery, disaster recovery, etc.	✓		FSA
15	The ED PIN will conform to Federal authentication standards. Any exceptions to Federal, Department of Education, or FSA policy will be documented.	✓		OMB
16	The ED PIN credential data is established through a 3rd party verification match with the U.S. Social Security Administration (SSA). The ED PIN system uses the SSA 3rd party verification functionality available in CPS.	✓	A B J	FSA
17	The ED PIN credential does not expire.	✓		FSA
18	The ED PIN record in the repository is not deleted.	✓		FSA
19	The ED PIN application is only available via the ED PIN site (www.pin.ed.gov) and not available via paper application or any other option except as authorized by the Department.	✓		FSA
20	For user authentication, the ED PIN requires use of the user's social security number, first 2 characters of the last name, date of birth and the ED PIN.	✓		FSA

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
21	Any action requiring user authentication on the ED PIN system will require the use of the ED PIN access credential for that user.	✓		FSA
22	All ED PIN authentication data is protected with access controls and encryption to prevent unauthorized individuals, including system administrators and customer support representatives, from obtaining the data.	✓		ISO / IEC
23	Any ED PIN access credential transmission (including between the components of the ED PIN system as well as user directories) requires that it be transmitted securely.	✓		FSA
24	The ED PIN will be protected as it is entered into any system including suppressing the display of the ED PIN as it is entered.	✓		ISO / IEC
25	Unsuccessful attempts in using the ED PIN access credentials will automatically deactivate the ED PIN for a specified duration.	✓		ISO / IEC
26	The ED PIN data will be administered by authorized personnel. The ED PIN data administration will include interfaces to other authorized FSA business processes utilizing the ED PIN.	✓		ISO / IEC
27	The ED PIN permits the use of 4 numeric or 6 alphabetic characters as the ED PIN. Sequential numbers are not permitted. 6 alphabetic characters are supported but not used for the issuance of new ED PINs.	✓		FSA
28	Under normal circumstances, the ED PIN is not required to be changed. The ED PIN may be changed by the user, may be disabled by the user and subsequently enabled by the user, and may be deactivated (including interruption of on-going user session) by the Department of Education under certain circumstances.	✓		FSA
29	A temporary (or Guest) ED PIN is not issued regardless of role.	✓		FSA
30	All users are notified not to use an easy-to-guess ED PIN,			

FEDERAL
STUDENT AID
We Help Put America Through School

FSA Integration Partner
ED PIN Re-Engineering Analysis
131.1.2 Business Requirements & Standards

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
	not to divulge their ED PIN, and not to store their ED PIN where others can find them.	✓		FSA
31	Advanced authentication (a challenge-response system) is used to allow users to disable their ED PIN and re-enable their ED PIN.	✓		ISO / IEC
32	Advanced authentication (such as cryptographic keys or tokens) is used for authorized system administration functions associated with any ED PIN component.	✓		ISO / IEC
33	Location based access to the ED PIN system is not permissible.	✓		ISO / IEC
34	The ED PIN cannot be communicated, securely or otherwise, in any way to any one (including administrators) other than the user. Communication of the ED PIN to the user is only permitted in a secure transmission.	✓		NIST
35	Users using the ED PIN will be informed why this type of authentication is used.	✓		OMB
36	Users will also be told what authorized FSA client system access is permitted with the ED PIN.	✓		NIST
37	An ED PIN is unique to support individual accountability and authentication. An ED PIN can not be issued to a group or organization. An ED PIN can not be issued anonymously.	✓		FSA
38	There are no roles associated with a user and their associated ED PIN. Any role-based authorization based on authentication with the ED PIN system is the responsibility of the business process using the ED PIN as an authentication service.	✓		FSA
39	The ED PIN system is available 24 X 7 X 365, within FSA service level agreements, except as authorized by the Department.	✓		FSA
40	There are no service constraints for users to use the ED PIN system (i.e., no restriction on how many times the system is used).	✓		NIST

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
41	The ED PIN system will not provide search capabilities to users.	✓		
42	All access to the ED PIN system will be monitored.	✓		ISO / IEC
43	Access to specific ED PIN functions for which users do not have access is never allowed.	✓		ISO / IEC
44	The ED PIN system physical infrastructure will be protected in compliance with Federal regulations. These protections include port protection, secure firewalls and gateways, intrusion detection, real-time monitoring, etc.	✓		NIST
45	The ED PIN system will possess the capability to send reminder notifications.	✓		FSA
46	Keystroke monitoring will not be utilized in any activity associated with the user's use of the ED PIN.	✓		ISO / IEC
47	Any ED PIN authentication data stored on client desktops must be encrypted. Permanent cookies with ED PIN authentication data are not permitted.	✓		NIST
48	The ED PIN system will not permit the retrieval of more than one ED PIN.	✓		FSA
49	Session management standards will comply with the Department policy. These standards will include new session established with a client every time an HTTP request reaches the ED PIN server, a session will be terminated at a pre-determined time interval after the last activity, etc.	✓		ISO / IEC
50	Only server-side data input validation is permitted.	✓		ISO / IEC
51	All users must be notified that the ED PIN system is a U.S. Government service and malicious activity may be monitored.	✓		OMB
52	The ED PIN system will not provide single sign-on functionality.	✓		FSA

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
	Use of the ED PIN access credential by any single sign-on process (including password synchronization, etc.) either internal or external to FSA will require prior approval from the ED PIN system owner. The ED PIN system will comply with the FSA Access and Enrollment Management Policy (in development).			
53	There are no restrictions for the number of times users may change their ED PIN on an active ED PIN access credential.	✓		ISO / IEC
54	The ED PIN system will allow batch registration (bulk processing) for user ED PINs from FSA client systems authorized to perform this functionality.	✓		FSA
55	Users will be notified by the authorized FSA client system submitting a registration request that an ED PIN will be requested on their behalf. There is variable text on the ED PIN e-mail notification and the ED PIN paper mailer that informs the recipient why the ED PIN was generated. While there is no advance notice given to a user in all instances, users will be provided an explanation upon receipt of the ED PIN.	✓		FSA
56	The ED PIN functionality is for individual use only. Any delegation associated with an individual ED PIN is not permitted.	✓		FSA
57	The ED PIN system design supports multi-vendor components.	✓		FSA
58	Use of the ED PIN in other authorized FSA systems is restricted to user authentication only. Administrative access to other FSA systems using the ED PIN is not permitted.	✓		FSA
59	In the event of an ED PIN system outage an alert message will be posted on the ED PIN web site.	✓		FSA
60	The end-user facing ED PIN authentication screens will comply with federal regulations for usability.	✓		NIST
61	Access scripts with embedded information are prohibited.	✓		ISO /

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
				IEC
62	Procedures for key management (encryption) exist for key generation, distribution, storage, use, destruction and archiving. The procedures associated with key management may be further strengthened particularly with segregation of responsibilities and maintenance of activity logs.	✓		ISO / IEC
63	The ED PIN privacy policy statement will be displayed on all user facing pages. Additionally, this functionality will be identified as a U.S. Government system warning users about unauthorized access, punishment, etc. upon entering the ED PIN site.	✓		ISO / IEC
64	The ED PIN site will meet the general requirements of Public Law 99-506 Reauthorization of the Rehabilitation Act of 1973, Section 508-Electronic Equipment Accessibility, October 1986; and Public Law 100-542 Telecommunication Accessibility Enhancement Act, October 1988.	✓		NIST
65	The ED PIN system will provide documented access alternatives for authentication functions in FSA client systems. These access alternatives will follow applicable industry standards.	✓	P	FSA – DLS FSA – E-Gov
66	The ED PIN system is the enterprise shared service for <u>authentication of user identity</u>.		C E I	FSA
67	The ED PIN system will possess capability for reliable date and time stamps for authentication requests.		H N	FSA
68	The ED PIN system will make First Name a mandatory field for registration.		E	FSA - NSLDS
69	The ED PIN data will be maintained through interfaces with users, FSA business processes and systems.		E M	ISO / IEC
70	The ED PIN system will institute a formal process to authorize use of ED PIN functions that includes documentation related to agreements, testing		L	ISO / IEC

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
	procedures, contacts, capacity plans, etc. The formal process will be annual and documentation will be reviewed by the ED PIN business owner for compliance with requirements and standards.			
71	Different implementations of electronic signatures will be documented.		K	FSA - AP
72	Any change to user's identification data will deactivate the current ED PIN associated with that user and require the generation of a new ED PIN. Changes to user's identification data may be initiated in any FSA business process related to the user.		C E M	FSA - AP
73	Users will be notified that any change to their identification data will automatically result in the issuance of a new ED PIN. Any change to user's identification data (SSN, DOB and Last Name) is not permissible in the ED PIN system regardless of source without a re-issuance of the associated ED PIN. Changes to user's identification data may be the result of user initiated activity or another FSA transaction associated with the user in another FSA system.		M	FSA
74	Duplicate SSNs will not be active.		M	FSA - AP
75	A notification will be sent to the user if FSA determines that their ED PIN has been compromised.		F	OMB
76	Interim role-based ED PINs may be requested to support FAA authentication (e.g. those issued without SSA verification).		A B O	FSA - AP
77	There will be segregation of responsibilities among system administrators.		H N	ISO / IEC
78	The deactivation (lock-out) period for the ED PIN will be configurable by the system owner.		P	ISO / IEC
79	The total number of failed ED PIN authentication attempts by a user, regardless of session, will be configurable.		P	ISO / IEC

NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
80	Internal access by authorized ED PIN system administrators will be logged and audited.		H N	ISO / IEC FSA - AP
81	The ED PIN reminder notification functionality will be available to FSA client systems.		G	FSA – DL
82	The ED PIN reminder notification functionality will allow options for near real-time or batch communications.		F	FSA – DLS FSA-DLC FSA - AP
83	The ED PIN may allow alphanumeric characters.			ISO / IEC
84	All authorized systems using the ED PIN authentication service will be notified of system problems, outage period and expected availability.		L	ISO / IEC FSA - NSLDS
85	The ED PIN requirements and standards will be maintained and enforced.		L	NIST
86	End user facing screens for authentication will require all ED PIN access credentials and the screens will be consistent in the use of the credentials regardless of system.		D	FSA - DLS
87	All external access will be logged and the type of access will be based on authorized permission to use a particular ED PIN system function.		H N	ISO / IEC FSA - AP
88	Host-based authentication to the ED PIN system is not permitted.		P	ISO / IEC

| NO.	BUSINESS REQUIREMENT / STANDARD	Current Functionality (✓)	Cross-Reference to Findings	Source
89	Certain ED PIN functions will utilize audit trail accountability. These functions will include any change to user information. The audit trail functionality will be configurable for number of changes.		H N	ISO / IEC
90	Access to the ED PIN audit logs will be strictly controlled. There will be segregation of responsibility between groups that administer the access control function and those who administer the audit trail.		H	ISO / IEC
91	Confidentiality of audit trail information will be protected.		H	OMB
92	Audit trail information will be reviewed and may utilize automated tools.		H	ISO / IEC
93	All ED PIN deactivations will be logged and reviewed by authorized personnel. Other appropriate security alerts will be defined in the ED PIN system security plan.		H N	ISO / IEC
94	Data integrity problems (duplicate records, security violations, etc.) over a particular configurable threshold (e.g., .0001%) in the ED PIN user repository will be considered serious and will trigger an audit. Availability of the ED PIN system during such audits will be decided by the ED PIN system owner.		M	ISO / IEC
95	Applicable demographic updates will be communicated among the ED PIN and FSA client systems.		C E	FSA - DLS

5 CONCLUSIONS

FSA should keep ED PIN simple (to use), scaleable (for user growth) and flexible (to allow for additional functional use). Use of COTS for this non-core FSA business enablement function should be considered. Three ED PIN areas for functional enhancement include:

1. Process & Integration (i.e., SSIM & functional consolidation)
   a. ED PIN should be an independent process and system rather than a sub system of CPS.
   b. The ED PIN should have minimal maintenance components to support its purpose.
   c. Interfaces with systems that use the ED PIN should be consistent in functionality.
2. Data Administration / Technology (i.e., roles/PIN activity)
   a. The ED PIN system should incorporate roles as part of the application process to distinguish the different types of users.
   b. The ED PIN system should allow specific functionality relative to the various roles.
   c. Use of the ED PIN system should be tracked for each function and system.
3. Evolving Standards (i.e., Federal and Industry IT security)
   a. The ED PIN system should use Federal and Industry authentication standards.

The ED PIN processes provide a simple and accepted way to authenticate users. The user's personal information and ED PIN can be used to gain access to several FSA systems regardless of their stage in the financial aid life cycle. While issuance of the ED PIN is not a core mission function of FSA, it provides the necessary business simplification aspect relative to authentication of users. Process automation capabilities and integration of the ED PIN processes and data with other FSA facilities will ensure its continued functionality. Adoption and implementation of the SSIM initiative guidance will also help enhance the quality of ED PIN authentication. Additionally, FSA can effectively manage risk through a continuously improving and standards-compliant approach. FSA's continued focus on service and performance will help achieve increased adoption of FSA electronic services where users can leverage their ED PIN. To ensure the operating scale necessary for use of the ED PIN it is imperative that FSA:

1. Institutionalize and communicate business requirements and standards,
2. Enhance the quality of the data in the ED PIN repository, and
3. Maintain currency with all industry IT security standards-based authentication approaches.
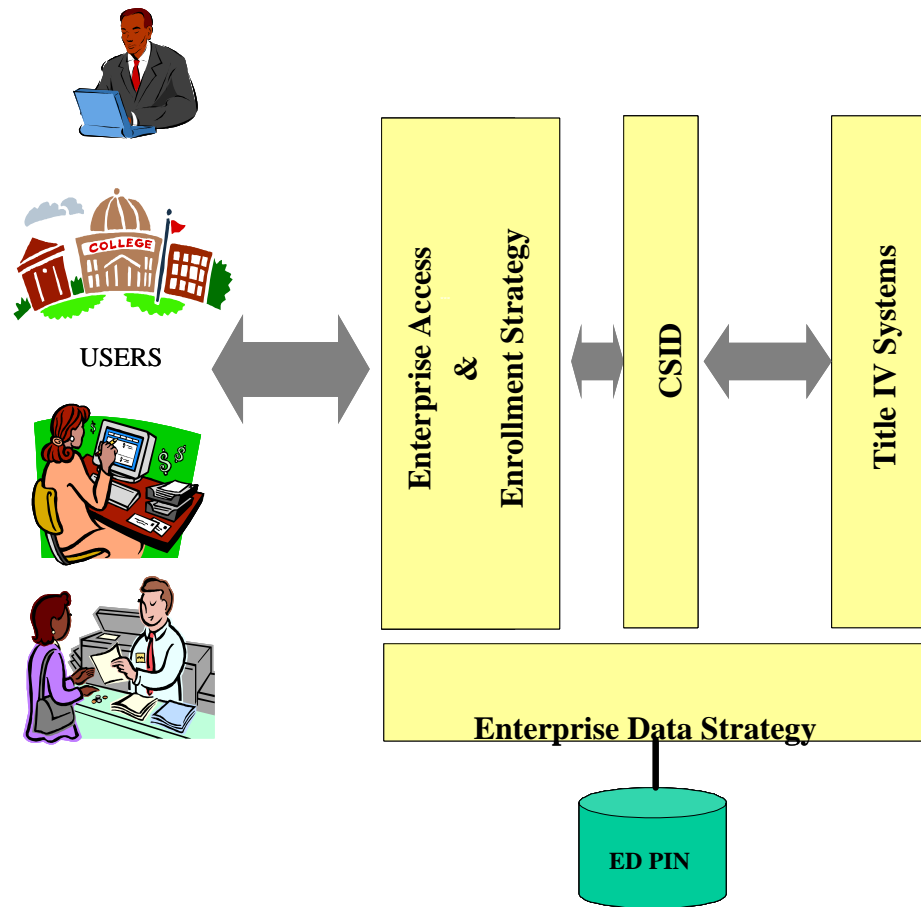
Conclusions from the ED PIN Re-Engineering Analysis include the following:

- Maintain Comprehensive ED PIN Business Requirements for the 6-functions:
  - Identification
  - Registration
  - Authentication
  - E-Signature
  - ED PIN Self Service
  - Administration, Management & Reporting
- Enforce adherence to ED PIN Standards
- Immediate ED PIN Data Administration activities to increase data quality
- Institute Data Management Controls; and includes implementation of SSIM guidelines, once approved

- Consolidate ED PIN functionality distributed across multiple systems based on a Risk Assessment and Cost Benefit Analysis including the potential alternative for a COTS solution (Enterprise Shared Service); continue to leverage SSA match from CPS
- Institute ECM Policies and regular Communications with all Stakeholders

The business requirements and standards noted in this document will form the basis of key aspects of the next phase. The objective of the next phase of this initiative - technical architecture upgrade analysis – is to develop a high level conceptual design for the re-engineered ED PIN system. This phase will also include an update for the ED PIN capacity plans.

6 REFERENCES

1. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-601 (PIN Web Site) thru Addendum 5.
2. The FSA PIN Overview.
3. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-602 (PIN Application Programming Interface) thru Addendum 1.
4. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-616 (PIN Application/PIN Address Correction) thru Addendum 1.
5. Report of PIN executions (Dec – March) for Update PIN, Update Address, Enable/Disable, Insert New PIN User, Reissue, Retrieve PIN, Select Record (no Dec data), Create Request (no Dec data), Check Request (no Dec data), and Authenticate.
6. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-610 Addendum #3.
7. FAFSA PIN Uses Document.
8. STAN Functional Specifications document, version 2.3, dated 2/14/2003, Tracker log #185.
9. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800-12. 1995
10. National Institute of Standards and Technology. *Minimum Security Requirements for Multi-User Operating Systems.* NISTIR 5153. March 1993.
11. Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force. *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information.* June 6, 1995.
12. U.S. Department of Education Strategic Plan 2002 – 2007.
13. National Institute of Standards and Technology. *Guidelines for the Security Certification and Accreditation of Federal Information Technology System.* Initial Public Draft, Version 1.0, October 2002.
14. E-Authentication Levels – Working Draft, OMB, March 2003.
15. FSA Proposed Business Justification. ED PIN Re-Engineering Analysis. March, 2003.
16. Generally Accepted System Security Principles (GASSP), I²SF, Version 2.0. June 1999.
17. FSA Integration Partner Deliverable 124.1.3, Security and Privacy Architecture Specification. May 2003.
18. FSA Integration Partner Deliverable 123.1.22, CSID *(renamed to SSIM)* High Level Design. May 2003.
19. Common Criteria for Information Technology Security Evaluation (ISO/IEC Standard 15408), version 2.1, August 1999.
20. Identity Theft: Greater Awareness and Use of Existing Data Are Needed. GAO-02-766 June 28, 2002.
21. Identity Theft: Prevalence and Cost Appear to be Growing. GAO-02-363 March 2002.
22. Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing. GAO-03-322 April 2003.

23. ID Theft: When Bad Things Happen to Your Good Name. Federal Trade Commission. September 2002.

APPENDIX A: CURRENT ED PIN PROCESSES / SYSTEMS / INTERFACES

ED PIN AS-IS High Level Logical Overview
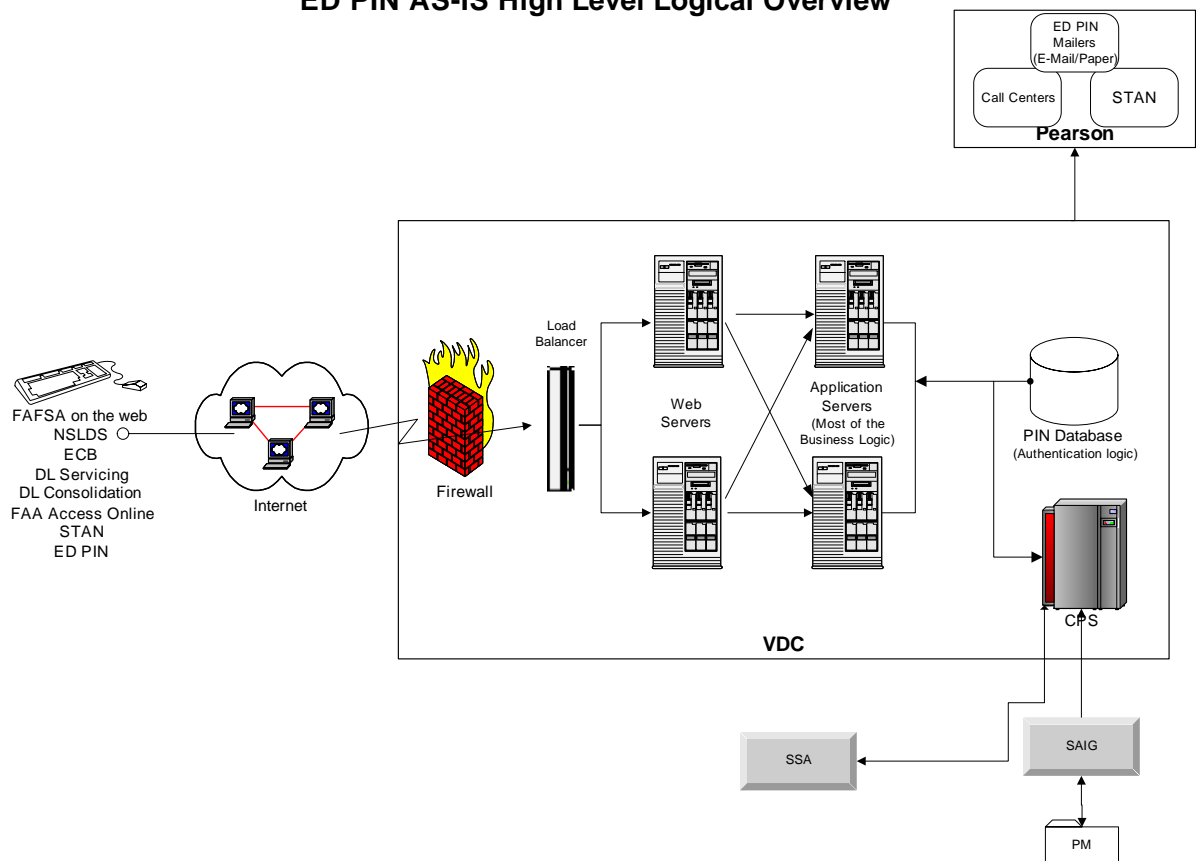
The ED PIN system is utilized by the following FSA business processes:

- FAFSA on the Web - for accessing renewal applications and electronic signature associated with any FAFSA on the Web product (i.e., original, renewal or correction application).
- STAN 1 – for electronic signature functions requiring audit log. STAN 2 does not use the ED PIN.
- NSLDS – for authentication of users.
- ECB – for authentication of FAAs.
- DL Servicing Center – for authentication of users.
- DL Consolidation - for authentication of users.

- DL Origination – for authentication of users and Promissory Note electronic signature function.
- FAA Access Online – for authentication of FAAs.

Other uses of the ED PIN:

- E-Servicing IVR – FSA has developed this capability using the ED PIN to authenticate users. This service (E-Servicing IVR) has not been deployed into production and currently there are no plans to do so.
- CSB (potential planned acquisition) - for authentication of users.
- E-Gov (future pilot with DHHS) - planned future authentication of users and/or electronic signature function.
- ED PIN - for authentication of users

System	Communication	Functions	NOTES
FAFSA on the web	Stored Procedure		
		Electronic Signature	ED PIN used as signature for electronically signing the applications
		Renewal FAFSA and Corrections	ED PIN used for verification to allow access to previously entered or submitted FAFSA data. CPS will perform an address check, and update the PIN DB based on most current date.
		Student Access	ED PIN used to authenticate user to view their transaction(s).
		Paper FAFSA processing	- CPS will submit a PIN application request if User does not have a PIN - CPS will update PIN address based on most current date
ED PIN Site			32,914,510 - Total records on db 23,674,859 - Total records with PIN 8,697 - Deactivated ED PIN's Approx. 20,000 ED PIN's issued to FAAs.
	FTP	Apply for PIN (Through PIN Site, CPS, PM)	If there is no current ED PIN record, required information is SSN, FN,

System	Communication	Functions	NOTES
			LN, MI, DOB and Mailing address for SSA Match, e-mail & pass-phrase are optional. CPS sends the information to SSA for verification. Validated records are forwarded to the PIN DB.
		Request	Request existing PIN (SSN, LN, DOB required)
		Change PIN	Change current PIN to a personalized PIN. SSN, LN, DOB, & Current PIN are needed for identification. To have the system regenerate a random PIN, only SSN, LN, and DOB is needed.
		Change PIN Information	Request existing SSN, LN, and DOB. Ability to change: FN, PIN mailing address, or e-mail address.
		Check Status	Verify PIN addresses and last day PIN was sent
		Disable	Must supply SSN, DOB, LN, & mother's maiden name to disable
		Re-enable	Must supply SSN, DOB, LN, & mother's maiden name to re-activate
		Check PIN Information	View PIN information
		Authentication	Performs PIN authentication
		Authentication Select	Performs select on tbl_auth by hash, also checks pin, used when users are updating their PIN to a number of their choice
		Sending PIN's	On the PIN DB, new PIN's are batched together twice daily to be sent to CPS. Transactions without e-mail address – generation of paper ED PIN mailers.
		E-mail handling	Business logic for handling e-mail ED PIN notifications

System	Communication	Functions	NOTES
			not viewed within 14 days
STAN	Stored Procedure		Direct connection to the ED PIN database.
		Electronic Signature	ED PIN used as a signature
		Perkins Promissory Notes	All signing of promissory notes use STAN; STAN provides the audit trail functionality necessary for this function.
		Federal Direct or Federal Family Education Loan (FFEL) Master Promissory Note	All signing of promissory notes use STAN; STAN provides the audit trail functionality necessary for this function.
FAA Access Online	PIN API		
		View students' SAR data	View a student's Student Aid Report (SAR) information, including the Expected Family Contribution (EFC), NSLDS information, SAR Comments, etc
		Check the status of batches	Check the status of batches submitted to the CPS for application or correction processing for a particular award year. You can view these batches sorted by: Federal School Code or ISIR Type/Batch Type
		Request the signature hold file and set the frequency of receipt	Receive a list of students for your school whose applications are on hold pending receipt of signature(s); determine how often schools may want to receive the signature hold file
		Application/Correction Entry	Enter a student's FAFSA, Renewal FAFSA or FAFSA Corrections on the Web form and submit it to CPS for processing
		Restore a Saved Application	Restore a partially completed and saved FAFSA, Renewal FAFSA or FAFSA Corrections on the

System	Communication	Functions	NOTES
			Web form and submit it to CPS for processing
NSLDS	PIN API		
		View Users Record	The site displays information on loan and/or grant amounts, outstanding balances, loan statuses, and disbursements.
ECB	PIN API		Used by school employees
		Submit FISAP information	Allows schools to submit information for Federal Perkins Loan, Federal Supplemental Educational Opportunity Grant (FSEOG), and Federal Work-Study (FWS) programs.
		Access Campus-Based account data	
		View reports	Schools can view the following Reports: - Accounting Transaction History - Statement of Account - Reports Incomplete - Reports No Submitted FISAP - Hold Schools Listing - Reports ELC 1 - Reports ELC 2 - Master Listing - Default Rate Comparison
DL Servicing	WebService		DL Servicing website sets a global variable which is passed throughout the session, and allows a user to view any secure section of the web site
	FTP	Batch File to Update Demographics	A PIN is required to update demographic info on DL servicing. Updated addresses are sent to check against a time stamp on the ED PIN DB to update the PIN site to the most current address. Syntax checking will be done on CPS, before

System	Communication	Functions	NOTES
			the batch file reaches the PIN DB.
			SSN is used as the Primary Key
DL Consolidation			Track the processing status of your online Consolidation Loan application throughout the entire consolidation process from application receipt to booking with Direct Loan Servicing
Other			
	Flat File daily (M-F) from SAIG / Participation Management (PM) to CPS	CPS receives the file to perform basic data validation, and then CPS automatically forwards all valid records to the PIN DB, address is updated based on current date of information.	User registers on PM. Records are sent through SAIG, then CPS to the PIN DB. No SSA match is done and record is given a PIN. For updates, the PIN DB can be updated, but not the CPS DB.
	FTP	E-mail handling (Leapfrog) & USPS	CPS performs syntax check (record counts, e-mail validity) on batched PIN's that are to be sent out to Pearson/Leapfrog.
	MQ Series (EAI) w/ Application Servers	Communication of ED PIN from CPS to ED PIN server.	MQ Series is only used for the PIN application process via the PIN website.

APPENDIX B: DEFINITION OF TERMS

Acceptable Risk – A concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls.

Accountability – Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation.

Adequate Security – Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Authentication – Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Availability – Assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service.

Component – An IT assembly, or part thereof, that is essential to the operation of some larger IT assembly and is an immediate subdivision of the IT assembly to which it belongs, (e.g., a trusted guard, biometrics device, or firewall would be a component of a computer system).

Confidentiality – Assurance that information in an IT system is not disclosed to unauthorized persons, processes, or devices.

Configuration Management – A family of security controls in the management class dealing with the control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IT system.

Contingency Planning – A family of security controls in the operations class dealing with emergency response, backup operations, and post-disaster recovery for an IT system, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Criticality/Sensitivity – A measure of the importance and nature of the information processed, stored, and transmitted by the IT system to the organization's mission and day-to-day operations.

Data Integrity – Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.

Designated Approving Authority – Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

Developer – The organization or individual that develops the IT system.

Environment – Aggregate of external procedures, conditions, and objects affecting the development, operation and maintenance of an IT system.

Exposure – A measure of the potential risk to an IT system from both external and internal threats.

External System Exposure – Relates to: (1) the method by which users access the system, (e.g., dedicated connection, intranet connection, Internet connection, wireless network), (2)

the existence of backend connections to the system and to what the backend systems are connected, and (3) the number of users that access the system.

Firmware – Program recorded in permanent or semi permanent computer memory.

Identification – The process of ascertaining an individual's identity or confirming that the purported identity is correct. Identification relies on one or more of three factors: something an individual has, something an individual knows, and something an individual is (such as signature or biometric attribute).

Identification and Authentication – A family of security controls in the technical class dealing with ensuring that users are individually authenticated via passwords, tokens, or other devices, and that access controls to the IT system are enforcing segregation of duties.

Individual Accountability – Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

IT Security – Information operations protect and defend information and IT systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IT systems by incorporating protection, detection and reaction capabilities.

IT System – The set of agency information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Categories of IT systems are major applications and general support systems.

Integrity – Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

Internal System Exposure – Relates to the types of individuals that have authorization to access the system and the information the system stores, processes, and transmits. It includes such items as individual security background assurances and/or clearance levels, access approvals, and need-to-know.

Logical Access – A family of security controls in the technical class dealing with ensuring that logical access controls on the IT system restrict users to authorized transactions and functions.

Non-Repudiation – Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Operational Controls – Controls that address security mechanisms primarily implemented and executed by people (as opposed to systems).

Residual Risk – Portion of risk remaining after security controls have been applied.

Risk – The net mission impact considering: (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular IT system vulnerability and (2) the resulting impact if this should occur. IT system-related risks arise from legal liability or mission loss due to: (1) unauthorized (malicious or accidental) disclosure, modification, or destruction of information, (2) unintentional errors and omissions, (3) IT

disruptions due to natural or man-made disasters, and (4) failure to exercise due care and diligence in the implementation and operation of the IT system.

Risk Assessment – The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of risk management and synonymous with risk analysis.

Subsystem – A major subdivision or component of an IT system consisting of hardware/software/firmware that performs a specific function.

System – A generic term used for briefness to mean either a major application or a general support system.

System and Data Integrity – A family of security controls in the operations class dealing with the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data.

User – Person or process authorized to access an IT system.

Vulnerability – A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the systems security policy.

APPENDIX C: MEETING NOTES

<table>
<tr>
<td colspan="3"><h2 align="center">ED PIN Re-Engineering Analysis</h2><p align="center">June 9, 2003
Meeting Minutes</p></td>
</tr>
<tr>
<td>Attendees:
6/9 09:00am
At UCP</td>
<td colspan="2">Nina Colón   Yateesh Katyal   Pearson Gov't. Solutions (conference call)
Application Processing   DL Servicing (C. Battle & team)   ACS</td>
</tr>
<tr>
<td>Purpose of Meeting</td>
<td colspan="2"><u>Purpose</u>: Requirements/Standards meeting with Direct Loan (DL) Servicing
Agenda
1. Systems using the ED PIN – for authentication, other functions.
2. Type of access to the ED PIN.
3. Issues and/or strengths associated with the use of the ED PIN.
4. Future or anticipated requirements.</td>
</tr>
<tr>
<td>Decisions Made</td>
<td colspan="2">N/A.</td>
</tr>
<tr>
<td>Issues/Concerns</td>
<td colspan="2">See discussion items below.</td>
</tr>
<tr>
<td>Action Items</td>
<td>❑ Follow up meetings with technical teams to obtain documentation of ED PIN interface(s) and volume data:
    ❑ DL Servicing
    ❑ DL Consolidation
    ❑ Application Processing
❑ Neil Sattler requested a list of current business processes supported using the ED PIN.</td>
<td>Colón/ Katyal

Colón</td>
</tr>
<tr>
<td><u>Open</u> Action Items from Previous Meeting(s)</td>
<td colspan="2">N/A.</td>
</tr>
<tr>
<td>Next Meeting
1. TBD 34D1 (TO Status)
2. TBD Follow-up Meetings
3. 6/17 11am NSLDS</td>
<td colspan="2">1. Task Order status.
2. Follow-up meeting for ED PIN interface documentation and volume data with DL Servicing, DL Consolidation, and Application Processing.
3. NSLDS Requirements Meeting</td>
</tr>
<tr>
<td>Discussion Items

A. Direct Loan Servicing
B. Direct Loan Consolidation</td>
<td colspan="2">A. <u>Direct Loan Servicing</u>
Project background, objectives and schedule information was provided by the ED PIN Re-Engineering team (Katyal and Colón).
▪ The DL Servicing system uses the ED PIN to authenticate customers.
▪ The E-Servicing IVR is not in production; no current plans for implementation.</td>
</tr>
</table>

Consolidation **C. Application Processing**	implementation. - The DL Servicing system will implement Web Services ED PIN authentication in mid-July; testing in progress with Pearson. - Demographic updates on the DL Servicing system require ED PIN authentication. - Demographic updates on ED PIN do not require ED PIN for authentication. - Demographic updates on the DL Servicing system not communicated to ED PIN. - Demographic updates on the ED PIN not communicated to the DL Servicing system. - Largest ED PIN client following FOTW. - SSN is primary key in DL Servicing. - ED PIN generates a new record if stable data changed; DL Servicing maintains single record. - Address updates are made to the ED PIN record if address date is newer. - ED PIN does not offer choice of receiving ED PIN via USPS or e-mail. - Existence of e-mail address in DL Servicing not communicated to ED PIN. - CSRs do not request ED PIN; customers directed to ED PIN site. - Potential DL Servicing issue with Joint Consolidation business process. - DL Servicing would like customers to receive ED PIN faster. - DL Servicing would like capability to send ED PIN reminder prior to graduation from school. Follow-up meeting to be scheduled for ED PIN interface documentation and volume data with DL Servicing team. **B. <u>Direct Loan Consolidation</u>** Project background, objectives and schedule information was provided by the ED PIN Re-Engineering team (Katyal and Colón). - Borrowers access the DL Consolidation system for (1) loan application status and (2) e-signature of consolidation applications. - Most borrowers remain with the DL Consolidation process for a very short duration prior to moving on the DL Servicing stage. - Biggest problem is borrowers at consolidation stage do not possess ED PIN since it was not available at time of initial application contact with them. - Joint electronic signature is not available. DL consolidation also discourages joint consolidation. - Monthly volume is typically less than 10,000 customers. Follow-up meeting to be scheduled for ED PIN interface documentation and volume data with DL Consolidation team; specifically, Judy Weimer of EDS (502-326-1912) per authorization from Denise Leifeste.

C. <u>Application Processing</u>
Project background, objectives and schedule information was provided by the ED PIN Re-Engineering team (Katyal and Colón).

- Application Processing includes the following systems:
    - Central Processing System (CPS)
    - FAFSA on the Web (FOTW)
    - ED PIN
    - FAA Access Online
    - STAN (for electronic signature)
- Use of the ED PIN is not tracked other than in STAN.
- FAA Access functionality is increasing. Return to Title IV Funds functionality may extend the use of the ED PIN authentication for FAA Access to users other than FAAs in Schools. Same with SSCRs.
- Multiple ED PINs are generated due to stable data changes.
- Should a customer be forced to change their ED PIN at some stage?
- Forgotten ED PINs should be sent to customers in real-time.
- Future use of the ED PIN as an authentication mechanism may be extended to Title VII and Title VIII federal student aid programs as part of the E-Gov initiative.
- CPS does not use the ED PIN to authenticate users.
- The use of ED PIN Web Service is not planned for any Application Processing system.
- There is no audit/log associated with the electronic signature on FOTW.
- Neil Sattler suggested the following:
    - Maintain relationship of an ED PIN to records in multiple systems.
    - FSA should remain open to leveraging a single federal database (potentially other than ED PIN) to authenticate individuals.
    - Maintenance of standards.
    - Incorporate OIG audit results expected in a week.

A follow-up meeting will be scheduled to receive interface documentation and volume data.

FEDERAL
STUDENT AID
We Help Put America Through School

FSA Integration Partner
ED PIN Re-Engineering Analysis
131.1.2 Business Requirements & Standards

Documentation Library	1. **CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-601 (PIN Web Site) thru Addendum 5.** 2. The FSA PIN Overview. 3. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-602 (PIN Application Programming Interface) thru Addendum 1. 4. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-616 (PIN Application/PIN Address Correction) thru Addendum 1. 5. Report of PIN executions (Dec – March) for Update PIN, Update Address, Enable/Disable, Insert New PIN User, Reissue, Retrieve PIN, Select Record (no Dec data), Create Request (no Dec data), Check Request (no Dec data), and Authenticate. 6. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-610 Addendum #3. 7. FAFSA PIN Uses Document. 8. STAN Functional Specifications document, version 2.3, dated 2/14/2003, Tracker log #185.

ED PIN Re-Engineering Analysis
June 17, 2003
Meeting Minutes

Attendees: **6/9 09:00am** **At UCP**	Nina Colón Sandra Fowler Yateesh Katyal Pearson Gov't. Solutions (Pat Struve - conference call) Raytheon (Jim Snyder - conference call)
Purpose of Meeting	**Purpose**: Requirements/Standards meeting for **NSLDS**. Agenda 5. Systems using the ED PIN – for authentication, other functions. 6. Type of access to the ED PIN. 7. Issues and/or strengths associated with the use of the ED PIN. 8. Future or anticipated requirements.
Decisions Made	N/A.
Issues/Concerns	See discussion items below.

Action Items	❑ NSLDS – Raytheon will provide the following information:
	    1. Statistics associated with ED PIN downtime.
	    2. Volume data regarding use of ED PIN, with peak times if available.
	    3. Documentation on how session state is maintained (to ascertain if ED PIN data is used). Jim Snyder

Open Action Items from Previous Meeting(s)	❑ Follow up meetings with technical teams to obtain documentation of ED PIN interface(s) and volume data: Colón/Katyal
	    ❑ DL Servicing
	    ❑ DL Consolidation
	    ❑ Application Processing
	❑ Neil Sattler requested a list of current business processes supported using the ED PIN. Colón

Next Meeting 1. TBD 34D1 (TO Status) 2. TBD Follow-up Meetings	1. Task Order status. 2. Follow-up meeting for ED PIN interface documentation and volume data with DL Servicing, DL Consolidation, and Application Processing. 3. Meetings with Business Integration Group, Security Architecture and Architecture Working Group.
Discussion Items	Project background, objectives and schedule information was provided by the ED PIN Re-Engineering Analysis team (Colón and Katyal). ▪ NSLDS has 2 web sites. ▪ One web site is for Students and the other is for Financial Aid Professionals. ▪ The Students web site uses the ED PIN site for authentication and requires the users SSN, 1st 2 letters of the last name, date of birth and

	the ED PIN.
	▪ The Financial Aid Professionals web site has its own authentication specific to NSLDS.
	▪ The Students web site can be used for Inquiry purpose only.
	▪ Upon successful login (i.e., authentication with the ED PIN site) Students are presented with the NSLDS home page and a variety of other options. The home page provides a status of all loans associated with that user.
	▪ NSLDS uses the SSN/1st 2 letters of last name/DOB as the primary key. NSLDS keeps track of the user including name changes and also maintains alias tables. NSLDS maintains a names history.
	▪ Reliability of the ED PIN site is very important to NSLDS. There have been instances in the past where users have complained that NSLDS is not functioning when in fact the API has not been functioning or the ED PIN site has been down. The NSLDS team agreed to provide additional information to the ED PIN Re-Engineering Analysis.
	▪ The NSLDS team recommended the use of first name since that experiences less changes than the last name and is more reliable.
	▪ NSLDS is not authorized to update ED PIN data.
	▪ NSLDS does not perform any matching algorithm on the authentication process; only on data feeds to NSLDS.
Documentation Library	9. **CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-601 (PIN Web Site) thru Addendum 5.**
	10. The FSA PIN Overview.
	11. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-602 (PIN Application Programming Interface) thru Addendum 1.
	12. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-616 (PIN Application/PIN Address Correction) thru Addendum 1.
	13. Report of PIN executions (Dec – March) for Update PIN, Update Address, Enable/Disable, Insert New PIN User, Reissue, Retrieve PIN, Select Record (no Dec data), Create Request (no Dec data), Check Request (no Dec data), and Authenticate.
	14. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-610 Addendum #3.
	15. FAFSA PIN Uses Document.
	16. STAN Functional Specifications document, version 2.3, dated 2/14/2003, Tracker log #185.